

# ON MODULES OF INTEGRAL ELEMENTS OVER FINITELY GENERATED DOMAINS

KHOA D. NGUYEN

**ABSTRACT.** This paper is motivated by the results and questions of Jason P. Bell and Kevin G. Hare in [BH09]. Let  $\mathcal{O}$  be a finitely generated  $\mathbb{Z}$ -algebra that is an integrally closed domain of characteristic zero. We investigate the following two problems:

- (A) Fix  $q$  and  $r$  that are integral over  $\mathcal{O}$ , describe all pairs  $(m, n) \in \mathbb{N}^2$  such that  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ .
- (B) Fix  $r$  that is integral over  $\mathcal{O}$ , describe all  $q$  such that  $\mathcal{O}[q] = \mathcal{O}[r]$ .

In this paper, we solve Problem (A), present a solution of Problem (B) by Evertse and Györy, and explain their relation to the paper of Bell and Hare. In the following,  $c_1$  and  $c_2$  are effectively computable constants with a very mild dependence on  $\mathcal{O}$ ,  $q$ , and  $r$ . For (B), Evertse and Györy show that there are  $N \leq c_2$  elements  $s_1, \dots, s_N$  such that  $\mathcal{O}[s_i] = \mathcal{O}[r]$  for every  $i$ , and for every  $q$  such that  $\mathcal{O}[q] = \mathcal{O}[r]$ , we have  $q - us_i \in \mathcal{O}$  for some  $1 \leq i \leq N$  and  $u \in \mathcal{O}^*$ . This immediately answers two questions about Pisot numbers by Bell and Hare [BH09]. For (A), we show that except for some “degenerate” cases that can be explicitly described, there are at most  $c_1$  such pairs  $(m, n)$ . This significantly strengthens some results in [BH09]. We also make some remarks on effectiveness and discuss further questions at the end of the paper.

## 1. INTRODUCTION

Throughout this paper,  $\mathbb{N}$  denotes the set of positive integers. For simplicity, the terminology *finitely generated domain* means an integral domain of characteristic 0 finitely generated as an algebra over  $\mathbb{Z}$ . Fix an embedding  $\mathbb{Q} \subset \mathbb{C}$ . A Pisot number is a real algebraic integer greater than 1 whose other conjugates are of modulus less than 1. In [BH09], an algebraic integer  $q$  of degree  $d \geq 2$  over  $\mathbb{Q}$  is of full rank if the multiplicative group of  $\mathbb{C}^*$  generated by the conjugates of  $q$  either has rank  $d$ , or has rank  $d - 1$  and the norm of  $q$  is  $\pm 1$ . The following very interesting results are established in [BH09] (also see [BH12]):

- (i) Fix an algebraic integer  $q$  of full rank and positive integer  $n$ , the set of  $m \in \mathbb{N}$  such that  $\mathbb{Z}[q^m] = \mathbb{Z}[q^n]$  is finite ([BH09, Theorem 1.1]).
- (ii) Let  $q$  and  $r$  be full rank algebraic integers of degree  $d \geq 2$ . Then except certain explicit “degenerate” cases, the set of  $m \in \mathbb{N}$  such that  $\mathbb{Z}[q^m] = \mathbb{Z}[r^m]$  is finite ([BH09, Theorem 1.3]).
- (iii) Fix an algebraic integer  $r$  such that  $\mathbb{Q}(r)/\mathbb{Q}$  is Galois, there are only finitely many Pisot numbers  $q$  such that  $\mathbb{Z}[q] = \mathbb{Z}[r]$  ([BH09, Theorem 1.6]).

---

*Date:* Apr 20, 2015.

*2010 Mathematics Subject Classification.* Primary: 11D61; Secondary: 11R99.

*Key words and phrases.* unit equations over finitely generated domains, uniform bounds, effective methods.

Bell and Hare also ask two questions involving part (iii): is it possible to give a bound depending on  $r$  and to remove the assumption on  $\mathbb{Q}(r)/\mathbb{Q}$ ?

From now on,  $\mathcal{O}$  denotes an integrally closed finitely generated domain with fraction field  $K$ . The typical and most important examples are rings of integers in number fields. In our main result, we fix  $q$  and  $r$  that are integral over  $\mathcal{O}$  such that  $q^n$  and  $r^n$  are not in  $\mathcal{O}$  for every  $n \in \mathbb{N}$ , and study the equation  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  in both variables  $(m, n)$ . Our result significantly strengthen the above results in (i) and (ii) of Bell and Hare [BH09] at one stroke. When  $\mathcal{O} = \mathbb{Z}$  as in [BH09], it is obvious that the condition of being full rank implies the very mild condition  $\{q^n, r^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ . This latter condition is assumed in order to simplify the statements of our results stated in this section. It comes from the minor inconvenience that  $\mathcal{O}[t] = \mathcal{O}$  for every  $t \in \mathcal{O}$  no matter how large the “height” of  $t$  is. We will also explain how our arguments could handle the case when some  $q^n$  or  $r^n$  is in  $\mathcal{O}$  (see Section 5), hence provide a complete (in a certain *qualitative* sense) solution to the problem of describing  $(m, n)$  such that  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  even without the above condition on  $q$  and  $r$ . A remarkable feature of our result is that it provides a uniform bound with a very mild dependence on the data  $(\mathcal{O}, q, r)$  illustrated below (see Remark 1.3).

A theorem of Roquette [Roq58] (also see [Lan83, Chapter 2]) states that the group of units in a finitely generated domain is finitely generated. Hence  $\mathcal{O}^*$  has only finitely many torsion points. In other words, there are only finitely many roots of unity in  $K$ . We need the following:

**Definition 1.1.** Let  $\alpha$  be integral over  $\mathcal{O}$ . We say that  $\alpha$  is a unit over  $\mathcal{O}$  if  $N_{K(\alpha)/K}(\alpha) \in \mathcal{O}^*$ , where  $N_{K(\alpha)/K}$  is the norm map with respect to  $K(\alpha)/K$ . By using the minimal polynomial of  $\alpha$  over  $K$ , this is equivalent to requiring that  $\alpha$  is a unit in  $\mathcal{O}[\alpha]$ .

**Definition 1.2.** Let  $\alpha$  and  $\beta$  be integral over  $\mathcal{O}$ . The notation  $d(\mathcal{O}, \alpha, \beta)$  denotes the maximum of all the following numbers:

- (a)  $[K(\alpha) : K]$  and  $[K(\beta) : K]$ .
- (b) The rank of the group of units of  $\mathcal{O}[\sigma(\alpha), \sigma(\beta), \tau(\alpha), \tau(\beta)]$  for any two  $K$ -embeddings  $\sigma$  and  $\tau$  of  $K(\alpha, \beta)$  into  $\bar{K}$ .
- (c) The number of roots of unity in  $K$ .

Although the definition of  $d(\mathcal{O}, \alpha, \beta)$  looks somewhat complicated, we have the following simple observation:

*Remark 1.3.* If  $K$  is a number field,  $S$  is a finite set of places of  $K$  containing all the archimedean ones,  $\mathcal{O}$  is the ring of  $S$ -integers of  $K$ , and  $\alpha$  and  $\beta$  are integral over  $\mathcal{O}$ , then  $d(\mathcal{O}, \alpha, \beta)$  could be bounded explicitly in terms of  $\max\{[K(\alpha) : \mathbb{Q}], [K(\beta) : \mathbb{Q}]\}$  and the cardinality of  $S$ . This follow from (the  $S$ -unit version of) Dirichlet’s unit theorem.

Before stating our main result, we need to define subsets of  $\mathbb{N}^2$  corresponding to certain “degenerate” cases (this name comes from degenerate solutions of certain unit equations considered later). Let  $q$  and  $r$  be integral over  $\mathcal{O}$  such that  $\{q^n, r^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ . Define the subsets  $\mathcal{A}_{\mathcal{O}, q, r}$ ,  $\mathcal{B}_{\mathcal{O}, q, r}$ ,  $\mathcal{C}_{\mathcal{O}, q, r}$  as follows:

$$\mathcal{A}_{\mathcal{O}, q, r} := \{(m, n) \in \mathbb{N}^2 : \frac{q^m}{r^n} \in \mathcal{O}^*\},$$

$$\mathcal{B}_{\mathcal{O},q,r} := \{(m,n) \in \mathbb{N}^2 : [K(r^n) : K] = 2 \text{ and } \frac{q^m}{\sigma(r^n)} \in \mathcal{O}^*\}$$

where  $\sigma$  in the definition of  $\mathcal{B}_{\mathcal{O},q,r}$  is the nontrivial automorphism of the quadratic extension  $K(r^n)/K$ . Finally, if  $q$  and  $r$  are units over  $\mathcal{O}$ , we define:

$$\mathcal{C}_{\mathcal{O},q,r} := \{(m,n) \in \mathbb{N}^2 : q^m r^n \in \mathcal{O}^*\};$$

otherwise define  $\mathcal{C}_{\mathcal{O},q,r} = \emptyset$ . By our assumption on  $q$  and  $r$ , we have  $\mathcal{A}_{\mathcal{O},q,r} \cap (\mathcal{B}_{\mathcal{O},q,r} \cup \mathcal{C}_{\mathcal{O},q,r}) = \emptyset$ . On the other hand, when  $r$  is a unit over  $\mathcal{O}$ , we have  $\mathcal{B}_{\mathcal{O},q,r} \subseteq \mathcal{C}_{\mathcal{O},q,r}$ .

Obviously, if  $(m,n) \in \mathcal{A}_{\mathcal{O},q,r}$  then  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ . If  $(m,n) \in \mathcal{B}_{\mathcal{O},q,r}$ , note that  $[K(r^n) : K] = 2$  and let  $\sigma$  denote the nontrivial  $K$ -automorphism of  $K(r^n)$ . Using the fact that  $r^n + \sigma(r^n) \in \mathcal{O}$ , we have that  $\mathcal{O}[q^m] = \mathcal{O}[\sigma(r^n)] = \mathcal{O}[r^n]$ . Finally, if  $(m,n) \in \mathcal{C}_{\mathcal{O},q,r}$ , put  $u = q^m r^n \in \mathcal{O}$ . Using the minimal polynomials of  $r^n$  and  $q^m$  over  $K$ , we have  $q^m = \frac{u}{r^n} \in \mathcal{O}[r^n]$  and  $r^n = \frac{u}{q^m} \in \mathcal{O}[q^m]$  hence  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ .

Because of this, the following result is, in a certain qualitative sense, best possible:

**Theorem 1.4.** *Let  $q$  and  $r$  be integral over  $\mathcal{O}$  such that  $\{q^n, r^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ . There is an effectively computable constant  $c_3$  depending only on  $d(\mathcal{O}, q, r)$  such that outside  $\mathcal{A}_{\mathcal{O},q,r} \cup \mathcal{B}_{\mathcal{O},q,r} \cup \mathcal{C}_{\mathcal{O},q,r}$  there are at most  $c_3$  pairs  $(m,n) \in \mathbb{N}^2$  satisfying  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ .*

The bound  $c_3$  as well as other similar bounds in this paper follow from work of Beukers and Schlickewei [BS96], and Evertse, Schlickewei, and Schmidt [ESS02] on unit equations together with some combinatorial arguments. Hence it is fairly straightforward to make them explicit although we do not provide all the details in doing so. Conceivably, all these bounds are far from optimal. In this paper, we do not spend any efforts to optimize them as long as they depend uniformly only on  $d(\mathcal{O}, q, r)$  instead of  $\mathcal{O}$ ,  $q$ , and  $r$ . Theorem 1.4 immediately implies the following (see Theorem 1.1 and Theorem 1.3 in [BH09]).

**Corollary 1.5.** *Let  $K$  be a number field with the ring of integers  $\mathcal{O}_K$ . Let  $q$  be an algebraic integer such that  $q^n \notin \mathcal{O}_K$  for every  $n \in \mathbb{N}$ . There is an effectively computable constant  $c_4$  depending only on  $[K(q) : \mathbb{Q}]$  such that there are at most  $c_4$  pairs  $(m,n) \in \mathbb{N}^2$  satisfying  $m \neq n$  and  $\mathcal{O}_K[q^m] = \mathcal{O}_K[q^n]$ .*

*Proof.* We apply Theorem 1.4 with  $r = q$  and  $\mathcal{O} = \mathcal{O}_K$ ; the resulting bound  $c_4$  only depends on  $[K(q) : \mathbb{Q}]$  thanks to Remark 1.3. By the assumption on  $q$ , the sets  $\mathcal{B}_{\mathcal{O},q,q}$  and  $\mathcal{C}_{\mathcal{O},q,q}$  are empty while the set  $\mathcal{A}_{\mathcal{O},q,q}$  is exactly the set of pairs  $(m,n)$  with  $m = n$ .  $\square$

**Corollary 1.6.** *Let  $q$  and  $r$  be algebraic integers. There is an effectively computable constant  $c_5$  depending only on  $\max\{[\mathbb{Q}(q) : \mathbb{Q}], [\mathbb{Q}(r) : \mathbb{Q}]\}$  such that the following holds. If there are more than  $c_5$  numbers  $n \in \mathbb{N}$  such that  $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$  then we have one of the following:*

- (a)  $\frac{q}{r}$  is a root of unity.
- (b)  $\frac{q}{r_1}$  is a root of unity for some conjugate  $r_1 \neq r$ . Moreover, this case can only happen if for some  $n \in \mathbb{N}$ , we have  $[\mathbb{Q}(r^n) : \mathbb{Q}] = 2$  and  $r_1^n \neq r^n$ .
- (c)  $qr$  is a root of unity.

*Proof.* We apply Theorem 1.4 when  $K = \mathbb{Q}$  and  $\mathcal{O} = \mathbb{Z}$ ; the resulting bound  $c_5$  only depends on  $\max\{[\mathbb{Q}(q) : \mathbb{Q}], [\mathbb{Q}(r) : \mathbb{Q}]\}$  by Remark 1.3. Since there are more

than  $c_5$  many  $n$  such that  $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$ , by Theorem 1.4 there is some  $n_0$  such that  $(n_0, n_0) \in \mathcal{A}_{\mathbb{Z}, q, r} \cup \mathcal{B}_{\mathbb{Z}, q, r} \cup \mathcal{C}_{\mathbb{Z}, q, r}$ . Cases (a), (b), and (c) respectively come from the cases where  $(n_0, n_0)$  belong to  $\mathcal{A}_{\mathbb{Z}, q, r}$ ,  $\mathcal{B}_{\mathbb{Z}, q, r}$  and  $\mathcal{C}_{\mathbb{Z}, q, r}$ .  $\square$

The previous corollaries strengthen results by Bell and Hare mentioned in parts (i) and (ii) at the beginning of this paper. For their questions asked in part (iii), we fix  $r$  which is integral over  $\mathcal{O}$  and study the collection of  $q$  satisfying the equation  $\mathcal{O}[q] = \mathcal{O}[r]$ . Evertse and Györy [EG85] prove that there exists a positive integer  $N$  uniformly bounded by an explicit quantity with a mild dependence on  $\mathcal{O}$  and  $r$  such that the following holds. There are  $s_1, \dots, s_N$  such that  $\mathcal{O}[s_i] = \mathcal{O}[r]$  for  $1 \leq i \leq N$  and for every  $q$  satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$ , we have  $q - us_i \in \mathcal{O}$  for some  $u \in \mathcal{O}^*$ . Furthermore, if  $\mathcal{O} \subseteq \bar{\mathbb{Q}}$  or if  $\mathcal{O}$  belongs to certain families of integrally closed finitely generated domains then Györy proves that a list  $\{s_1, \dots, s_N\}$  satisfying the above property can be determined effectively. We refer the readers to [Gyö84], [EG85] and the references there for more details. In Section 3, we briefly explain how to prove the above results by Györy and Evertse-Györy and why they immediately answer the questions by Bell and Hare.

To prove Theorem 1.4, we start with the equality  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  and its consequence that the discriminants of  $q^m$  and  $r^n$  over  $K$  differ by an element in  $\mathcal{O}^*$ . Then it is straightforward to obtain a list of solutions of the unit equation  $x + y + z = 1$  where  $x, y, z$  belong to a subgroup of  $\bar{K}^*$  whose rank is bounded in terms of  $d(\mathcal{O}, q, r)$ . A celebrated result of Evertse, Schlickewei and Schmidt [ESS02] provides a uniform bound for the number of nondegenerate solutions (i.e. when  $x, y, z \neq 1$ ). On the other hand, when many solutions are degenerate, it is not obvious to get out the exact relations as described in the definition of  $\mathcal{A}_{\mathcal{O}, q, r}$ ,  $\mathcal{B}_{\mathcal{O}, q, r}$ , and  $\mathcal{C}_{\mathcal{O}, q, r}$ . Some extra combinatorial and Galois theoretic arguments are needed for this remaining problem where we bound the number of degenerate solutions that are outside  $\mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$ . The proof of the results by Györy and Evertse on the equation  $\mathcal{O}[q] = \mathcal{O}[r]$  follows the same idea, but we have a simpler equation of the form  $x + y = 1$  in variables  $x, y$  instead. For this equation, there is an earlier result by Beukers and Schlickewei [BS96] that provides a reasonably good uniform bound on the number of solutions. Moreover, when  $x$  and  $y$  are taken inside a finitely generated subgroups of  $\bar{\mathbb{Q}}^*$ , the equation  $x + y = 1$  can be solved effectively using Baker's method or the Thue-Siegel principle (see, for example, [GY06] and [BG06, pp. 146–148]).

In the next section, we present results involving discriminants and, more importantly, the above results on unit equations. After that, we present briefly the work of Evertse and Györy on the equation  $\mathcal{O}[q] = \mathcal{O}[r]$  with a given  $r$ . Then we prove Theorem 1.4 and explain how to remove the very mild condition  $\{q^n, r^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$  assumed there. This provides a complete solution to the problem of describing all  $(m, n)$  such that  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  for any  $q$  and  $r$ . At the end, we discuss the effectiveness of the results in this paper and some related questions.

**Acknowledgments.** We wish to thank Professors Jason Bell, Mike Bennett, Jan-Hendrik Evertse, Dragos Ghioca, Kálmán Györy, Kevin Hare, and the anonymous referee for many helpful suggestions to improve the paper.

## 2. SOME PRELIMINARY RESULTS

**2.1. Discriminants.** Let  $A$  be an integrally closed domain with fraction field  $E$  of characteristic 0. For any  $\alpha$  algebraic over  $E$  of degree  $D$  with conjugates  $\alpha_0 =$

$\alpha, \dots, \alpha_{D-1}$  we define the discriminant of  $\alpha$  over  $E$  to be:

$$\text{disc}_E(\alpha) := \prod_{0 \leq i < j < D} (\alpha_i - \alpha_j)^2.$$

We have the following well-known result:

**Proposition 2.1.** *If  $\alpha$  and  $\beta$  are integral over  $A$  satisfying  $A[\alpha] = A[\beta]$  then  $\text{disc}_E(\alpha) = u \text{disc}_E(\beta)$  for some  $u \in A^*$ .*

*Proof.* See [Rib01, pp. 20–21]. Although the results there are stated over number fields, the proof can be carried over without any change. Integral closedness of  $A$  is needed for the fact that  $A[\alpha]$  (respectively  $A[\beta]$ ) is free with basis  $1, \alpha, \dots, \alpha^{D-1}$  (respectively  $1, \beta, \dots, \beta^{D-1}$ ) where  $D = [E(\alpha) : E] = [E(\beta) : E]$ .  $\square$

**2.2. Unit equations in 3 variables.** Fix  $n \geq 2$ , we start with the following:

**Definition 2.2.** *Let  $a_1, \dots, a_n \in \mathbb{C}^*$ . A solution  $(u_1, \dots, u_n) \in (\mathbb{C}^*)^n$  of the equation  $a_1x_1 + \dots + a_nx_n = 1$  in variables  $x_1, \dots, x_n$  is called nondegenerate if no subsums vanish. In other words, there is no proper subset  $\emptyset \neq J \subset \{1, \dots, n\}$  such that  $\sum_{j \in J} a_j u_j = 0$ .*

Equations of the form  $a_1x_1 + \dots + a_nx_n = 1$  where each  $x_i$  is an  $S$ -unit in a number field have played a fundamental role in diophantine geometry since work of Siegel in the 1920s. After many decades of intense activities, Evertse, Schlickewei and Schmidt obtained the following celebrated result with a remarkable uniform bound [ESS02, Theorem 1.1]:

**Theorem 2.3.** *Suppose  $\Gamma$  is a subgroup of  $(\mathbb{C}^*)^n$  of rank  $R$ . Consider the equation:*

$$a_1x_1 + \dots + a_nx_n = 1$$

*in variables  $x_1, \dots, x_n$ . Then the number of nondegenerate solutions in  $\Gamma$  is at most  $\exp((6n)^{3n}(R+1))$ .*

As a consequence, we have the following:

**Corollary 2.4.** *Let  $G$  be a subgroup of  $\mathbb{C}^*$  of rank  $R$ , there are at most  $\exp(18^9(3R+1))$  nondegenerate solutions  $(x_1, x_2, x_3) \in G^3$  of the equation  $x_1 + x_2 + x_3 = 1$ .*

**2.3. Unit equations in 2 variables.** The special case of Theorem 2.3 when  $n = 2$  was obtained earlier by Beukers and Schlickewei [BS96, Theorem 1.1]. It has the immediate consequence:

**Corollary 2.5.** *Let  $G$  be a subgroup of  $\mathbb{C}^*$  of rank  $R$ , there are at most  $2^{16R+16}$  solutions  $(x, y) \in G^2$  of the equation  $ax + by = 1$ .*

*Proof.* Let  $\Gamma = G \times G$  which has rank  $R^2$ . Beukers and Schlickewei [BS96, Theorem 1.1] consider the equation  $X + Y = 1$ . We can transform the given equation  $ax + by = 1$  into that equation by enlarging  $\Gamma$  with  $(a, 1)$  and  $(1, b)$ .  $\square$

Let  $h : \bar{\mathbb{Q}} \rightarrow \mathbb{R}_{\geq 0}$  be the absolute logarithmic Weil height (see [BG06, Chapter 1]). By using Baker's theory of linear forms in logarithms [Bak75], [BW93], [Yu07] or the Thue-Siegel principle [Bom93], [BC97], we can solve the equation  $ax + by = 1$  effectively when  $a, b \in \bar{\mathbb{Q}}^*$  and the variables  $x$  and  $y$  take values in a finitely generated subgroups of  $\bar{\mathbb{Q}}^*$ . The readers are referred to [GY06, Theorem 1], [BG06, pp. 146–148], and the references there for more details. We have:

**Theorem 2.6.** *Let  $a, b \in \bar{\mathbb{Q}}^*$  and  $G$  be a finitely generated subgroup of  $\bar{\mathbb{Q}}^*$ . There is an effectively computable constant  $c_6(a, b, G)$  depending on  $a$ ,  $b$ , and  $G$  such that every solution  $(x, y) \in G^2$  of  $ax + by = 1$  satisfies  $\max\{h(x), h(y)\} \leq c_6(a, b, G)$ .*

*Remark 2.7.* Recently, Evertse and Györy [EG13] showed that Theorem 2.6 still holds without the condition that  $a, b \in \bar{\mathbb{Q}}^*$  and  $G \subset \bar{\mathbb{Q}}^*$ . In their results, we need to express the finitely generated domain  $\mathbb{Z}[a, b, g_1, \dots, g_R]$  where  $g_1, \dots, g_R$  are generators of  $G$  into the form  $\mathbb{Z}[x_1, \dots, x_m]/I$  and replace the height function on  $\bar{Q}$  by a certain “size” function. We do not use this result here and refer the readers to [EG13].

### 3. RESULTS OF EVERTSE-GYÖRY AND QUESTIONS OF BELL-HARE

For the rest of this section, fix an integrally closed finitely generated domain  $\mathcal{O}$  with fraction field  $K$ . We need the following:

**Definition 3.1.** *Let  $\alpha$  be integral over  $\mathcal{O}$ . The notation  $d(\mathcal{O}, \alpha)$  denotes the maximum of the following*

- (a)  $[K(\alpha) : K]$
- (b) *The rank of the group of units of  $\mathcal{O}[\sigma(\alpha), \tau(\alpha)]$  for any two  $K$ -embeddings  $\sigma$  and  $\tau$  of  $K(\alpha)$  into  $\bar{K}$ .*

As before, we have the following:

*Remark 3.2.* If  $K$  is a number field,  $\mathcal{O}$  is the ring of  $S$ -integers in  $K$ , and  $\alpha$  is integral over  $\mathcal{O}$  then  $d(\mathcal{O}, \alpha)$  could be bounded explicitly in terms of  $[K(\alpha) : \mathbb{Q}]$  and the cardinality of  $S$ .

The following result is established by Györy [Gyö84] and Evertse-Györy [EG85]:

**Theorem 3.3** (Evertse-Györy). *Let  $r$  be integral over  $\mathcal{O}$ . There is an effectively computable constant  $c_7$  depending only on  $d(\mathcal{O}, r)$  such that the following holds. There are  $N \leq c_7$  numbers  $s_1, \dots, s_N$  such that  $\mathcal{O}[s_i] = \mathcal{O}[r]$  for  $1 \leq i \leq N$ , and for every  $q$  satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$ , we have  $q - us_i \in \mathcal{O}$  for some  $1 \leq i \leq N$  and some  $u \in \mathcal{O}^*$ . Moreover, when  $\mathcal{O} \subset \mathbb{Q}$ , such a list of  $s_1, \dots, s_N$  can be determined effectively.*

After a series of work, Györy [Gyö84] proved that there was such a *finite* list  $\{s_1, \dots, s_N\}$  and it could be determined effectively when  $\mathcal{O} \subset \mathbb{Q}$  or  $\mathcal{O}$  belonged to certain restricted classes of finitely generated domains. The assertion that  $c_7$  could be explicitly given and depended only on  $d(\mathcal{O}, r)$  was proved later by Evertse and Györy [EG85]. Strictly speaking, they represented  $\mathcal{O}$  and  $\mathcal{O}^*$  after choosing a transcendence basis and a finite set of valuations. Then they worked on the general theory of decomposable form equations and obtained a variant of Theorem 3.3 as an immediate consequence. In this section, we briefly explain the very simple aspects of their work by using the unit equation  $x + y = 1$  (or actually  $ax + by = 1$  with parameters  $(a, b)$ ) directly to obtain Theorem 3.3. We will avoid all the extra technical details for the more general decomposable form equations; the interested readers can refer to [Gyö84], [EG85] and the references there.

Before proving Theorem 3.3, we note the following immediate corollary which answers the two questions of Bell and Hare mentioned in (iii) at the beginning of this paper:

**Corollary 3.4.** *Fix an algebraic integer  $r \notin \mathbb{Z}$ . The number of Pisot numbers  $q$  satisfying  $\mathbb{Z}[q] = \mathbb{Z}[r]$  could be bounded uniformly in the degree of  $r$ . Moreover, all such Pisot numbers can be determined effectively.*

*Proof.* Apply Theorem 3.3 with  $\mathcal{O} = \mathbb{Z}$  and  $K = \mathbb{Q}$ , we obtain  $c_8$  depending only on  $[\mathbb{Q}(r) : \mathbb{Q}]$  (see Remark 3.2) such that there are  $N \leq c_8$  algebraic integers  $s_1, \dots, s_N$  satisfying the conclusion of Theorem 3.3. In particular, we have  $q = us_i + k$  for some  $1 \leq i \leq N$ ,  $u \in \{\pm 1\}$ , and  $k \in \mathbb{Z}$ . For a fixed  $i$  and  $u$ , there are at most two choices of  $k$  since we can pick a nontrivial embedding  $\sigma$  of  $\mathbb{Q}(r)$  into  $\bar{\mathbb{Q}}$  and use the fact that  $|\sigma(q)| = |\sigma(us) + k| < 1$ . Hence there are at most  $4c_8$  such Pisot numbers  $q$ . Since a list  $\{s_1, \dots, s_N\}$  can be determined effectively, so can the collection of all such Pisot numbers.  $\square$

*Remark 3.5.* There is nothing special about being a Pisot number in (the proof of) Corollary 3.4. The same arguments could be used for any collection of numbers  $q$  satisfying some appropriate boundedness condition that could be much weaker than conditions in the definition of Pisot numbers. For instance, we may consider the collection of  $q$  such that there is a nontrivial embedding  $\sigma$  of  $\mathbb{Q}(r)$  satisfying the condition that  $|\sigma(q)|$  is bounded above by a constant.

We now spend the rest of this section to prove Theorem 3.3. We may assume that  $r \notin K$ , otherwise Theorem 3.3 is obvious. Let  $L/K$  be the Galois closure of  $K(r)/K$ . For any two distinct  $K$ -embeddings  $\sigma$  and  $\eta$  of  $K$  into  $L$ , write  $\mathcal{O}_{\sigma,\eta} = \mathcal{O}[\sigma(r), \eta(r)]$ . For simplicity, write  $d = d(\mathcal{O}, r)$  and let  $c_9(d), c_{10}(d), \dots$  denote positive constants depending only on  $d$ . Let  $q$  be integral over  $\mathcal{O}$  such that  $\mathcal{O}[q] = \mathcal{O}[r]$ . We have that for every two distinct  $K$ -embeddings  $\sigma$  and  $\eta$  of  $K(r)$  into  $L$ , there is a unit  $u_{\sigma,\eta}$  of  $\mathcal{O}_{\sigma,\eta}^*$  such that:

$$(1) \quad \sigma(q) - \eta(q) = u_{\sigma,\eta}(\sigma(r) - \eta(r)).$$

**Case 1:**  $[K(r) : K] = 2$ . We can uniquely write  $q = a_0 + a_1 r$  with  $a_0, a_1 \in \mathcal{O}$ . By (1) with  $\sigma = \text{id}$  and  $\eta$  is the nontrivial  $K$ -automorphism of  $K(r)$ , we have that  $a_1 \in \mathcal{O}^*$ . This proves Theorem 3.3 and we may even take  $\{s_1, \dots, s_N\} = \{r\}$ .

**Case 2:**  $[K(r) : K] > 2$ . Let  $G_r$  be the subgroup of  $L^*$  generated by all the groups  $\mathcal{O}_{\sigma,\tau}^*$  and elements of the form  $\sigma(r) - \eta(r)$  for any two distinct  $K$ -embeddings  $\sigma$  and  $\tau$  of  $K(r)$  into  $L$ . By the definition of  $d = d(\mathcal{O}, r)$ , the rank of  $G_r$  is bounded by a constant  $c_9(d)$ .

For any two *distinct nontrivial*  $K$ -embeddings  $\sigma$  and  $\eta$ , Siegel's identity:

$$\frac{q - \sigma(q)}{\eta(q) - \sigma(q)} - \frac{q - \eta(q)}{\eta(q) - \sigma(q)} = 1$$

gives that:

$$(x_{q,\sigma,\eta}, y_{q,\sigma,\eta}) := \left( \frac{q - \sigma(q)}{\eta(q) - \sigma(q)}, -\frac{q - \eta(q)}{\eta(q) - \sigma(q)} \right)$$

is a solution of the unit equation  $x + y = 1$  to be solved for  $(x, y) \in G_r^2$ . Hence by Corollary 2.5, there is a finite set  $S_r \subseteq L^*$  whose cardinality is bounded above by a constant  $c_{10}(d)$  such that for every  $q$  satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$  and any two distinct nontrivial  $K$ -embeddings  $\sigma, \eta$  of  $K(r)$  into  $L$ , we have:

$$\left\{ \frac{q - \sigma(q)}{\eta(q) - \sigma(q)}, \frac{q - \eta(q)}{\eta(q) - \sigma(q)}, \frac{q - \sigma(q)}{q - \eta(q)} \right\} \subseteq S_r.$$

Now for any two pairs of distinct embeddings  $(\sigma_1, \eta_1)$  and  $(\sigma_2, \eta_2)$ , using:

$$\frac{\sigma_1(q) - \eta_1(q)}{\sigma_2(q) - \eta_2(q)} = \frac{(\sigma_1(q) - q) + (q - \eta_1(q))}{(\sigma_2(q) - q) + (q - \eta_2(q))}$$

we conclude that there are only finitely many possibilities for  $\frac{\sigma_1(q) - \eta_1(q)}{\sigma_2(q) - \eta_2(q)}$ .

Let  $d' = [K(r) : K]$  and  $\mathbb{P} := \mathbb{P}^{d'(d'-1)-1}$  with coordinates  $x_{(\sigma, \tau)}$  indexed by pairs  $(\sigma, \tau)$  of distinct  $K$ -embeddings of  $K(r)$  into  $L$ . We conclude that there is a finite set  $T_r \subseteq \mathbb{P}(L)$  whose cardinality is bounded above by a constant  $c_{11}(d)$  such that for every algebraic integer  $q$  satisfying  $\mathcal{O}_K[q] = \mathcal{O}_K[r]$ , the corresponding point  $((\sigma(q) - \eta(q)))_{(\sigma, \eta)}$  belongs to  $T_r$ .

Now if there are more than  $c_{11}(d)$  many  $q$  such that  $\mathcal{O}[q] = \mathcal{O}[r]$ , then there are at least two denoted by  $q$  and  $q^*$  such that the two points  $((\sigma(q) - \eta(q)))_{(\sigma, \eta)}$  and  $((\sigma(q^*) - \eta(q^*)))_{(\sigma, \eta)}$  in  $\mathbb{P}(L)$  coincide. In other words, there exists  $u \in L^*$  such that:

$$(2) \quad \frac{\sigma(q) - \eta(q)}{\sigma(q^*) - \eta(q^*)} = u \text{ for any distinct } \sigma \text{ and } \eta.$$

By (1), we have that  $u \in \mathcal{O}_{\sigma, \eta}^*$  for any distinct  $\sigma$  and  $\eta$ . Since  $K(r) = K(q) = K(q^*)$ , by lifting to  $\text{Gal}(L/K)$  we have:  $\frac{\tilde{\sigma}(q) - \tilde{\eta}(q)}{\tilde{\sigma}(q^*) - \tilde{\eta}(q^*)} = u$  for every  $\tilde{\sigma}, \tilde{\eta} \in \text{Gal}(L/K)$  such that  $\tilde{\sigma} \text{Gal}(L/K(r)) \neq \tilde{\eta} \text{Gal}(L/K(r))$ . This implies  $u$  is invariant under  $\text{Gal}(L/K)$ . Hence  $u \in \mathcal{O}^*$  thanks to integral closedness of  $\mathcal{O}$ . Now (2) with  $\sigma = \text{id}$  implies that the element  $q - uq^* \in K(r)$  is invariant under every  $K$ -embedding of  $K(r)$ . Hence  $q - uq^* \in \mathcal{O}$ . This proves the first assertion in Theorem 3.3.

For the remaining assertion, note that  $\mathcal{O} \subset \mathbb{Q}^*$  and  $K$  is now a number field. By Theorem 2.6 the finite sets  $S_r \subseteq L^*$  and  $T_r \subseteq \mathbb{P}(L)$  can be determined effectively. Now we fix a point  $(t_{(\sigma, \eta)}) \in T_r$  and show how to effectively determine all algebraic integers  $q$  such that  $\mathcal{O}[q] = \mathcal{O}[r]$  and the two points  $(\sigma(q) - \eta(q))$  and  $(t_{(\sigma, \eta)})$  in  $\mathbb{P}(L)$  coincide. In other words, we need to determine  $x \in L^*$  such that the system of equations:

$$(3) \quad \sigma(q) - \eta(q) = t_{(\sigma, \eta)} x \text{ for any } K\text{-embeddings } \sigma \neq \eta \text{ of } K(r)$$

could possibly yield a solution  $q$  satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$ .

Note that if  $x \in L^*$  is a choice such that (3) has a solution  $q$  satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$  then for every unit  $w \in \mathcal{O}^*$ ,  $xw$  is another choice with a solution  $qw$  of (3) satisfying  $\mathcal{O}_K[qw] = \mathcal{O}_K[r]$ . Hence it suffices to determine the images of all such  $x$  inside the quotient  $L^*/\mathcal{O}^*$ . Write  $t = \prod_{(\sigma, \eta)} t_{\sigma, \eta}$ . The system (3) together with Proposition 2.1 gives:

$$(4) \quad x^{d'(d'-1)} t \in \text{disc}_K(r) \mathcal{O}^*.$$

Denote  $(\mathcal{O}^*)^{d'(d'-1)} := \{w^{d'(d'-1)} : w \in \mathcal{O}^*\}$ . Let  $u_1, \dots, u_M \in \mathcal{O}_K^*$  be a choice of representatives for  $\mathcal{O}^*/(\mathcal{O}^*)^{d'(d'-1)}$ . To make such a choice, we simply need the group of roots of unity in  $K$  and a choice of generators for the “free part” of  $\mathcal{O}^*$ . This can be done effectively (compare Remark 3.6). Now (4) implies that

$$x \in \left( \frac{u_i \text{disc}_K(r)}{t} \right)^{1/(d'(d'-1))} \mathcal{O}^*$$

for some  $1 \leq i \leq M$ . Hence the list of possibilities for the image of  $x$  in  $L^*/\mathcal{O}^*$  can be effectively determined.



To finish the proof, given  $x \in L^*$ , we explain how to find all solutions  $q$  of (3) satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$ . Write

$$q = a_0 + a_1 r + \dots + a_{d'-1} r^{d'-1}$$

and we solve for  $(a_0, \dots, a_{d'-1})$  in the free  $\mathcal{O}$ -module  $\mathcal{O}^{d'}$  instead. Write  $t_\eta = t_{\sigma, \eta}$  if  $\sigma$  is the identity. Restrict (3) to the smaller system:

$$(5) \quad q - \eta(q) = t_\eta x \text{ for any nontrivial } K\text{-embedding } \eta \text{ of } K(r)$$

Then we have a linear system of  $(d' - 1)$  equations in the variables  $a_1, \dots, a_{d'-1}$ . The rows of the coefficient matrix  $C$  are of the form

$$(r - \eta(r), r^2 - \eta(r^2), \dots, r^{d'-1} - \eta(r^{d'-1}))$$

where  $\eta$  ranges over all nontrivial  $K$ -embeddings of  $K(r)$ . It is easy to see that  $C$  is invertible, as follows. Let  $D$  be the  $d' \times d'$  Vandermonde matrix whose rows are of the form:

$$(1, \eta(r), \dots, \eta(r)^{d'-1})$$

where  $\eta$  ranges over all (including the identity)  $K$ -embeddings of  $K(r)$ . In particular, the first row of  $D$  is  $(1, r, r^2, \dots, r^{d'-1})$ . By applying elementary column operations to transform the top row to  $(1, 0, \dots, 0)$ , we have that:

$$\det(D) = \pm \det(C).$$

Hence  $\det(C) \neq 0$ . Therefore there is a unique solution  $(a_1, \dots, a_{d'-1}) \in \mathbb{C}^{d'-1}$ . Now it depends on whether this unique solution  $(a_1, \dots, a_{d'-1})$  belongs to  $\mathcal{O}^{d'-1}$  and whether

$$q' = a_1 r + \dots + a_{d'-1} r^{d'-1}$$

satisfies  $\mathcal{O}[q'] = \mathcal{O}[r]$ . If that is the case, any  $q = a_0 + q'$  for any  $a_0 \in \mathcal{O}$  satisfies  $\mathcal{O}[q] = \mathcal{O}[r]$ . Otherwise, our initial choices of  $(t_{(\sigma, \tau)})$  and  $x$  do not yield any  $q$  satisfying  $\mathcal{O}[q] = \mathcal{O}[r]$ . Verifying the condition  $\mathcal{O}[q'] = \mathcal{O}[r]$  could be done effectively by, for example, checking if the change of coordinate matrices between  $\{1, q', \dots, q'^{d'-1}\}$  and  $\{1, r, \dots, r^{d'-1}\}$  is in  $\text{GL}_{d'}(\mathcal{O})$ . This finishes the proof of Theorem 3.3.

*Remark 3.6.* In fact, the sets  $S_r$  and  $T_r$  in the proof above can be determined effectively thanks to the results of Evertse and Györy [EG13] mentioned in Remark 2.7. However, we are grateful to Professor Evertse for the explanation that results in [EG13] are not enough to effectively determine a list  $\{s_1, \dots, s_N\}$  in Theorem 3.3 for an arbitrary integrally closed finitely generated domain  $\mathcal{O}$ . The problem is that in the above proof, we work with  $L^*/\mathcal{O}^*$ , hence require a list of generators of  $\mathcal{O}^*$ . When  $\mathcal{O} \subset \mathbb{Q}$  (i.e.  $\mathcal{O}$  is the ring of  $S$ -integers in a number field), generators of  $\mathcal{O}^*$  can be determined effectively. However, this is not known for a general  $\mathcal{O}$  (see [EG13, pp. 353]).

#### 4. PROOF OF THEOREM 1.4

**4.1. Notation and some preliminary results.** Throughout this section, fix an integrally closed finitely generated domain  $\mathcal{O}$  with fraction field  $K$ . Fix  $r$  and  $q$  that are integral over  $\mathcal{O}$  and satisfy  $\{r^n, q^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ . Let  $L$  denote the Galois closure of  $K(q, r)$ . Write  $d = d(\mathcal{O}, q, r)$  defined in Definition 1.2, and let  $c_{12}(d), c_{13}(d), \dots$  denote positive constants depending only on  $d$ . Define  $Q \in \mathbb{N}$

(respectively  $R \in \mathbb{N}$ ) to be the smallest positive integer satisfying  $K(q^Q) \subseteq K(q^n)$  (respectively  $K(r^R) \subseteq K(r^n)$ ) for every  $n \in \mathbb{N}$ . We have:

**Lemma 4.1.** *The exists a bound  $c_{12}(d)$  depending only on  $d$  for  $Q$  and  $R$ .*

*Proof.* In fact,  $Q$  and  $R$  are bounded above by the order  $s$  of the group of roots of unity in  $L^*$ , as follows. For every  $\sigma \in \text{Gal}(L/K)$ , if  $\sigma(q^Q) = q^Q$  then  $\sigma(q)/q$  is a root of unity. Hence we have  $\sigma(q^{Q-s}) = q^{Q-s}$ . This implies  $\text{Gal}(L/K(q^Q)) \subseteq \text{Gal}(L/K(q^{Q-s}))$ , and hence  $K(q^{Q-s}) \subseteq K(q^Q)$  violating the minimality of  $Q$  if  $Q > s$ . The same argument also shows  $R \leq s$ . Finally  $s$  could be bounded explicitly in terms of the number of roots of unity in  $K$  and  $[L : K]$ , hence in  $d$ .  $\square$

*Remark 4.2.* Note that the proof of Lemma 4.1 does *not* use the condition  $\{q^n, r^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ .

We need the following result for the proof of Theorem 1.4; it is a special case of Corollary 1.5.

**Proposition 4.3.** *There is a constant  $c_{13}(d)$  such that for every  $n_0 \in \mathbb{N}$ , there are at most  $c_{13}(d)$  many  $m \in \mathbb{N}$  (respectively  $n \in \mathbb{N}$ ) such that  $\mathcal{O}[q^m] = \mathcal{O}[q^{n_0}]$  (respectively  $\mathcal{O}[r^n] = \mathcal{O}[r^{n_0}]$ ).*

*Proof.* It suffices to prove the assertion involving the identity  $\mathcal{O}[q^m] = \mathcal{O}[q^{n_0}]$  since the other assertion involving  $\mathcal{O}[r^n] = \mathcal{O}[r^{n_0}]$  is completely analogous. We use the same idea as in the proof of Theorem 3.3. Since  $q^n \notin K$  for every  $n \in \mathbb{N}$ , there is  $\sigma \in \text{Gal}(L/K)$  such that  $\sigma$  does not fix  $q^n$  for every  $n \in \mathbb{N}$ . Suppose  $\mathcal{O}[q^m] = \mathcal{O}[q^{n_0}]$ , then there is a unit  $u_m$  of the ring  $\mathcal{O}[q, \sigma(q)]$  such that

$$q^m - \sigma(q^m) = u_m(q^{n_0} - \sigma(q^{n_0})).$$

Let  $G$  be the subgroup of  $L^*$  generated by the units in  $\mathcal{O}[q, \sigma(q)]$ ,  $q$  and  $\sigma(q)$ . Then the rank of  $G$  is bounded in terms of  $d$  only. We have that  $(u_m^{-1}q^m, -u_m^{-1}\sigma(q^m)) \in G^2$  is a solution of the equation:

$$\frac{1}{q^{n_0} - \sigma(q^{n_0})}(x + y) = 1.$$

By Corollary 2.5, there are at most  $c_{13}(d)$  possibilities for  $\frac{q^m}{\sigma(q^m)}$ .

Hence, if there are more than  $c_{13}(d)$  many  $m$  such that  $\mathcal{O}[q^m] = \mathcal{O}[q^{n_0}]$  then there are  $m_1 < m_2$  such that

$$\frac{q^{m_1}}{\sigma(q^{m_1})} = \frac{q^{m_2}}{\sigma(q^{m_2})}.$$

In other words,  $\sigma$  fixes  $q^{m_2-m_1}$ , contradicting the choice of  $\sigma$ .  $\square$

Finally, we have the following which can be proved using a similar idea:

**Proposition 4.4.** *There is a constant  $c_{14}(d)$  such that if  $K(r^R) \neq K(q^Q)$  then there are at most  $c_{14}(d)$  pairs  $(m, n) \in \mathbb{N}^2$  such that  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ .*

*Proof.* We may assume  $K(q^Q) \not\subseteq K(r^R)$ , hence  $\text{Gal}(L/K(r^R))$  is not a subgroup of  $\text{Gal}(L/K(q^Q))$ . Thus we can choose  $\sigma \in \text{Gal}(L/K(r^R))$  such that  $\sigma$  does not fix  $q^n$  for any  $n \in \mathbb{N}$ . Now it suffices to prove that there is a constant  $c_{15}(d)$  such that for every fixed  $0 \leq \ell \leq R-1$  there are at most  $c_{15}(d)$  finitely many pairs  $(m, n)$  satisfying  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  and  $n \equiv \ell$  modulo  $R$ . Once this is done, the desired  $c_{14}(d)$  can be taken to be  $Rc_{15}(d)$  (note Lemma 4.1).

For every such  $(m, n)$ , write  $n = \tilde{n}R + \ell$ . As before, there is a unit  $u_{m,n}$  of the ring  $\mathcal{O}[q^m, \sigma(q^m), r^n, \sigma(r^n)] \subseteq \mathcal{O}[q, \sigma(q), r, \sigma(r)]$  such that:

$$q^m - \sigma(q^m) = u_{m,n}(r^n - \sigma(r^n)) = u_{m,n}r^{\tilde{n}R}(r^\ell - \sigma(r^\ell)).$$

Let  $G$  be the subgroup of  $L^*$  generated by the units of the ring  $\mathcal{O}[q, \sigma(q), r, \sigma(r)]$ ,  $q$ ,  $\sigma(q)$ , and  $r$ . Then the rank of  $G$  is bounded in terms of  $d$  only. We have that  $\left(\frac{q^m}{u_{m,n}r^{\tilde{n}R}}, -\frac{\sigma(q^m)}{u_{m,n}r^{\tilde{n}R}}\right) \in G^2$  is a solution of the equation:

$$\frac{1}{r^\ell - \sigma(r^\ell)}(x + y) = 1.$$

By Corollary 2.5, there is a constant  $c_{16}(d)$  such that there are at most  $c_{16}(d)$  possibilities for  $\frac{q^m}{\sigma(q^m)}$ .

Recall the constant  $c_{13}(d)$  in Proposition 4.3, define  $c_{15}(d) := c_{13}(d)c_{16}(d)$ . Now if there are more than  $c_{15}(d)$  pairs  $(m, n)$  with  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  and  $n \equiv \ell$  modulo  $R$ , then Proposition 4.3 implies that those pairs yield  $N > c_{16}(d)$  many pairs denoted  $(m_1, n_1), \dots, (m_N, n_N)$  such that  $m_1, \dots, m_N$  are distinct. We may assume  $m_1 < \dots < m_N$ . By the property of  $c_{16}(d)$  as the upper bound for the possibilities of  $\frac{q^m}{\sigma(q^m)}$ , there exist  $1 \leq i < j \leq N$  such that:

$$\frac{q^{m_i}}{\sigma(q^{m_i})} = \frac{q^{m_j}}{\sigma(q^{m_j})}.$$

In other words,  $\sigma$  fixes  $q^{m_j - m_i}$ , contradicting the choice of  $\sigma$ . This finishes the proof.  $\square$

**4.2. Proof of Theorem 1.4.** By Proposition 4.4, we may assume that  $K(q^Q) = K(r^R)$ ; denote this field by  $K^o$ . As in the proof of Proposition 4.4, it suffices to fix  $k, \ell$  with  $0 \leq k \leq Q - 1$  and  $0 \leq \ell \leq R - 1$ , and show that there are at most  $c_{17}(d)$  pairs  $(m, n) \notin \mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$  satisfying  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ ,  $m \equiv k$  modulo  $Q$ , and  $n \equiv \ell$  modulo  $R$ . Once this is done, the desired constant  $c_3(d)$  in the conclusion of Theorem 1.4 can be taken to be  $QRc_{17}(d)$  (note Lemma 4.1). The convenience of doing this is that we can fix  $F := K(q^k) = K(q^m) = K(r^n) = K(r^\ell)$ . We have the following tower of fields:

$$K \subsetneq K^o \subseteq F \subseteq L.$$

Define:

$$W_{k, \ell} := \{(m, n) \in \mathbb{N}^2 : \mathcal{O}[q^m] = \mathcal{O}[r^n], m \equiv k \pmod{Q}, \text{ and } n \equiv \ell \pmod{R}\}.$$

Let  $G$  be the subgroup of  $L^*$  generated by the units of the rings  $\mathcal{O}[q, \sigma(q), r, \sigma(r)]$  for all  $\sigma \in \text{Gal}(L/K)$  and by all the conjugates of  $q$  and  $r$  over  $K$ . As in the proof of Theorem 3.3, for every  $(m, n) \in W_{k, \ell}$  and every  $\sigma \in \text{Gal}(L/K) \setminus \text{Gal}(L/F)$  there is a unit  $u_{m, n, \sigma}$  of the ring  $\mathcal{O}[q, \sigma(q^m), r, \sigma(r^n)] \subseteq \mathcal{O}[q, \sigma(q), r, \sigma(r)]$  such that

$$0 \neq q^m - \sigma(q^m) = u_{m, n, \sigma}(r^n - \sigma(r^n)).$$

Therefore  $\mathbf{x}_{m, n, \sigma} := \left(\frac{q^m}{\sigma(q^m)}, -\frac{u_{m, n, \sigma}r^n}{\sigma(q^m)}, \frac{u_{m, n, \sigma}\sigma(r^n)}{\sigma(q^m)}\right)$  is a solution of the unit equation

$$(6) \quad x + y + z = 1 \text{ with } (x, y, z) \in G^3.$$

Note that  $\mathbf{x}_{m,n,\sigma} = \mathbf{x}_{m,n,\tau}$  and  $u_{m,n,\sigma} = u_{m,n,\tau}$  if the two cosets  $\sigma \text{Gal}(L/F)$  and  $\tau \text{Gal}(L/F)$  coincide. Since the rank of  $G$  is bounded in terms of  $d$  only, by Corollary 2.4, the number of nondegenerate solutions is at most  $c_{18}(d)$ . We have the following:

**Lemma 4.5.** *Let  $\sigma \text{Gal}(L/F)$  be a coset in  $\text{Gal}(L/K)$  with  $\sigma \notin \text{Gal}(L/K^o)$ , there are at most  $c_{18}(d)$  many  $(m, n) \in W_{k,\ell}$  such that the solution  $\mathbf{x}_{m,n,\sigma}$  of (6) is nondegenerate.*

*Proof.* Assume there are more than  $c_{18}(d)$  pairs  $(m, n) \in W_\ell$  such that  $\mathbf{x}_{m,n,\sigma}$  is degenerate. Recall that  $c_{18}(d)$  is a bound on the number of solutions of (6), hence there are two distinct pairs  $(m_1, n_1)$  and  $(m_2, n_2)$  such that

$$(7) \quad \mathbf{x}_{m_1, n_1, \sigma} = \mathbf{x}_{m_2, n_2, \sigma}.$$

We may assume  $m_1 \neq m_2$ , the case  $n_1 \neq n_2$  is completely analogous. Without loss of generality, assume  $m_1 < m_2$ . Equation (7) implies:

$$\frac{q^{m_1}}{\sigma(q^{m_1})} = \frac{q^{m_2}}{\sigma(q^{m_2})}.$$

In other words,  $\sigma$  fixes  $q^{m_2-m_1}$ . Note that  $m_2 \equiv m_1 \equiv k$  modulo  $Q$ . Hence the field  $K(q^{m_2-m_1}) \subseteq K^o$  is fixed by  $\sigma$  and any element of  $\text{Gal}(L/K^o)$ . Since  $\sigma \notin \text{Gal}(L/K^o)$ , the field  $K(q^{m_2-m_1})$  is strictly smaller than  $K^o = K(q^Q)$ , contradicting the choice of  $Q$ .  $\square$

There are precisely  $[F : K] - [F : K^o] < d$  cosets  $\sigma \text{Gal}(L/F)$  in  $\text{Gal}(L/K)$  with  $\sigma \notin \text{Gal}(L/K^o)$ . We define  $c_{19}(d) := dc_{18}(d)$ . We now complete the proof of Theorem 1.4 by showing that there are at most  $c_{19}(d)$  pairs  $(m, n)$  in  $W_{k,\ell} \setminus (\mathcal{A}_{\mathcal{O},q,r} \cup \mathcal{B}_{\mathcal{O},q,r} \cup \mathcal{C}_{\mathcal{O},q,r})$ . Assume there are more than  $c_{19}(d)$  such pairs. By Lemma 4.5, there exists a pair  $(\tilde{m}, \tilde{n}) \in W_{k,\ell} \setminus (\mathcal{A}_{\mathcal{O},q,r} \cup \mathcal{B}_{\mathcal{O},q,r} \cup \mathcal{C}_{\mathcal{O},q,r})$  such that the solution  $\mathbf{x}_{\tilde{m}, \tilde{n}, \sigma}$  of (6) is degenerate for *every* coset  $\sigma \text{Gal}(L/F)$  in  $\text{Gal}(L/K)$  with  $\sigma \notin \text{Gal}(L/K^o)$ . We will show that this is impossible.

For any coset  $\sigma \text{Gal}(L/F)$  with  $\sigma \notin \text{Gal}(L/K^o)$ , degeneracy of  $\mathbf{x}_{\tilde{m}, \tilde{n}, \sigma}$  falls into one of the following two types (note that we always have  $\sigma(q^{\tilde{m}}) \neq q^{\tilde{m}}$  since  $\sigma \notin \text{Gal}(L/F)$ ):

- Type I:  $q^{\tilde{m}} = u_{\tilde{m}, \tilde{n}, \sigma} r^{\tilde{n}}$  and  $u_{\tilde{m}, \tilde{n}, \sigma} \sigma(r^{\tilde{n}}) = \sigma(q^{\tilde{m}})$ . This implies that  $\sigma$ , hence every element in the coset  $\sigma \text{Gal}(L/F)$ , fixes  $\frac{q^{\tilde{m}}}{r^{\tilde{n}}}$ .
- Type II:  $q^{\tilde{m}} = -u_{\tilde{m}, \tilde{n}, \sigma} \sigma(r^{\tilde{n}})$  and  $-u_{\tilde{m}, \tilde{n}, \sigma} r^{\tilde{n}} = \sigma(q^{\tilde{m}})$ . This implies that  $\sigma$ , hence every element in the coset  $\sigma \text{Gal}(L/F)$ , fixes  $q^{\tilde{m}} r^{\tilde{n}}$ .

Note that it is possible that both types happen for the same coset  $\sigma \text{Gal}(L/F)$ . Let  $H_1 := \text{Gal}\left(L/K\left(\frac{q^{\tilde{m}}}{r^{\tilde{n}}}\right)\right)$  and  $H_2 := \text{Gal}(L/K(q^{\tilde{m}} r^{\tilde{n}}))$ . We have proved the following:

$$(8) \quad \text{Gal}(L/K) = \text{Gal}(L/K^o) \cup H_1 \cup H_2.$$

We need the following well-known lemma in group theory:

- Lemma 4.6.** (a) *A group cannot be the union of two proper subgroups.*  
 (b) *If a group  $A$  is the union of three proper subgroups  $A_1, A_2$ , and  $A_3$  then  $[A : A_i] = 2$  for  $1 \leq i \leq 3$ ,  $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3$  is a normal subgroup of  $A$  and the quotient is isomorphic to the Klein four-group.*

*Proof.* Part (a) is an easy exercise. Part (b) is a classical result attributed to Scorza. See, for example, [BBM70] for a proof.  $\square$

Then we have:

**Lemma 4.7.**  *$\text{Gal}(L/K)$  is equal to  $H_1$  or  $H_2$ , but not both.*

*Proof.* Assume both  $H_1$  and  $H_2$  are proper subgroups of  $\text{Gal}(L/K)$  (note that  $\text{Gal}(L/K^o)$  is a proper subgroup by the assumption on  $q$  and  $r$ ), then Lemma 4.6 implies that  $\text{Gal}(L/K^o)$ ,  $H_1$ , and  $H_2$  are distinct subgroups of index 2 in  $\text{Gal}(L/K)$ .

Hence the fields  $K^o$ ,  $K\left(\frac{q^{\tilde{m}}}{r^{\tilde{n}}}\right)$ ,  $K(q^{\tilde{m}}r^{\tilde{n}})$  are distinct fields of degree 2 over  $K$ . Since the elements  $\left(\frac{q^{\tilde{m}}}{r^{\tilde{n}}}\right)^{QR}$  and  $(q^{\tilde{m}}r^{\tilde{n}})^{QR}$  belong to the intersection of  $K^o$  with each of the remaining 2 fields, they belong to  $K$ . Hence  $q^{2\tilde{m}QR}$  is in  $K$ , contradiction. Hence  $\text{Gal}(L/K) = H_1$  or  $\text{Gal}(L/K) = H_2$ .

The last assertion is easy: suppose  $\text{Gal}(L/K) = H_1 = H_2$ , then both  $\left(\frac{q^{\tilde{m}}}{r^{\tilde{n}}}\right)$  and  $q^{\tilde{m}}r^{\tilde{n}}$  belong to  $K$ . Hence  $q^{2\tilde{m}} \in K$ , contradiction.  $\square$

We can now complete the proof of Theorem 1.4 by showing that  $(\tilde{m}, \tilde{n})$  must belong to  $\mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$ . We divide into 2 cases:

**Case 1:**  $\text{Gal}(L/K) = H_1$ . This gives  $\frac{q^{\tilde{m}}}{r^{\tilde{n}}} \in K$ . We claim that there must be at least one coset  $\sigma \text{Gal}(L/F)$  with  $\sigma \notin \text{Gal}(L/K^o)$  such that the degeneracy of  $\mathbf{x}_{\tilde{m}, \tilde{n}, \sigma}$  falls into Type I. Otherwise if every degeneracy is of Type II, we have  $\text{Gal}(L/K) = \text{Gal}(L/K^o) \cup H_2$  and Lemma 4.6 gives that  $\text{Gal}(L/K) = H_2$  contradicting Lemma 4.7. Pick such a coset  $\sigma \text{Gal}(L/F)$  as claimed, then  $\frac{q^{\tilde{m}}}{r^{\tilde{n}}} = u_{\tilde{m}, \tilde{n}, \sigma}$  is a unit in  $\mathcal{O}[q, \sigma(q), r, \sigma(r)]$ . Hence  $\frac{q^{\tilde{m}}}{r^{\tilde{n}}} \in \mathcal{O}^*$ ; in other words  $(\tilde{m}, \tilde{n}) \in \mathcal{A}_{\mathcal{O}, q, r}$ .

**Case 2:**  $\text{Gal}(L/K) = H_2$ . This gives  $\alpha := q^{\tilde{m}}r^{\tilde{n}} \in \mathcal{O}$ . By arguing as in Case 1, we can choose a coset  $\eta \text{Gal}(L/F)$  such that  $\eta \notin \text{Gal}(L/K^o)$  and the degeneracy of  $\mathbf{x}_{\tilde{m}, \tilde{n}, \eta}$  falls into Type II. Denoting  $d' = [F : K]$ , we can uniquely write:

$$q^{\tilde{m}} = a_0 + a_1 r^{\tilde{n}} + \dots + a_{d'-1} r^{\tilde{n}(d'-1)}$$

for  $a_0, \dots, a_{d'-1} \in \mathcal{O}$ . Therefore:

$$\alpha = q^{\tilde{m}}r^{\tilde{n}} = a_0 r^{\tilde{n}} + \dots + a_{d'-1} r^{\tilde{n}d'}.$$

Since  $d' = [K(r^{\tilde{n}}) : K]$ , we must have  $a_{d'-1} \neq 0$  and

$$X^{d'} + \frac{a_{d'-2}}{a_{d'-1}} X^{d'-1} + \dots + \frac{a_0}{a_{d'-1}} X - \frac{\alpha}{a_{d'-1}}$$

is the minimal polynomial of  $r^{\tilde{n}}$  over  $K$ . In particular:

$$(9) \quad \frac{\alpha}{a_{d'-1}} = \pm N_{F/K}(r^{\tilde{n}}).$$

where  $N_{F/K}$  denotes the norm map associated to the extension  $F/K$ . This implies:

$$(10) \quad q^{\tilde{m}} = \frac{\alpha}{r^{\tilde{n}}} = \frac{\pm N_{F/K}(r^{\tilde{n}}) a_{d'-1}}{r^{\tilde{n}}}.$$

Our choice of the coset  $\eta \text{Gal}(L/F)$  gives:

$$(11) \quad q^{\tilde{m}} = -u_{\tilde{m}, \tilde{n}, \eta} \eta(r^{\tilde{n}})$$

Together with (10), we have:

$$(12) \quad \pm N_{F/K}(r^{\tilde{n}}) a_{d'-1} = u_{\tilde{m}, \tilde{n}, \eta} r^{\tilde{n}} \eta(r^{\tilde{n}}).$$

We now have two subcases:

**Case 2.1:**  $d' = [F : K] = 2$ , then  $\eta(r^{\tilde{n}})$  is the conjugate of  $r^{\tilde{n}}$  that is different from  $r^{\tilde{n}}$ . Equation (12) gives that  $a_{d'-1} = \pm u_{\tilde{m}, \tilde{n}, \eta}$  is a unit in the ring  $\mathcal{O}[q, \eta(q), r, \eta(r)]$ . Since  $a_{d'-1} \in \mathcal{O}$ , we have that  $a_{d'-1} \in \mathcal{O}^*$ . Finally, equation (10) gives that  $q^{\tilde{m}} = u\eta(r^{\tilde{n}})$  for a unit  $u \in \mathcal{O}^*$ . This means  $(\tilde{m}, \tilde{n}) \in \mathcal{B}_{\mathcal{O}, q, r}$ .

**Case 2.2:**  $d' = [F : K] > 2$ . Equation (12) implies that  $a_{d'-1} \in \mathcal{O}^*$  and some conjugate of  $r^{\tilde{n}}$  is a unit over  $\mathcal{O}$  (see Definition 1.1), hence  $r^{\tilde{n}}$  itself is also a unit over  $\mathcal{O}$ . Finally equation (10) gives that  $q^{\tilde{m}} r^{\tilde{n}} \in \mathcal{O}^*$ . This means  $(\tilde{m}, \tilde{n}) \in \mathcal{C}_{\mathcal{O}, q, r}$ .

In conclusion, we have the contradiction that  $(\tilde{m}, \tilde{n}) \in \mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$ . Hence the set

$$W_{k, \ell} \setminus (\mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r})$$

must have at most  $c_{19}(d)$  elements. This gives at most  $QRc_{19}(d)$  pairs  $(m, n) \in \mathbb{N}^2$  outside  $\mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$  satisfying  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ . Lemma 4.1 finishes the proof of Theorem 1.4.

## 5. AN ADDENDUM TO THEOREM 1.4

For the sake of completeness, we explain how to describe all pairs  $(m, n)$  such that  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  without the condition that  $\{q^n, r^n : n \in \mathbb{N}\} \cap \mathcal{O} = \emptyset$ . This section, though somewhat lengthy due to various cases to be considered, is rather elementary. The notations  $d, L, Q$ , and  $R$  are as in the beginning of Section 4.1. Without loss of generality, we assume that  $r^R \in \mathcal{O}$ . We consider two cases.

**5.1. The case  $q^Q \notin \mathcal{O}$ .** For every  $0 \leq \ell \leq R-1$ , define:

$$W_\ell := \{(m, n) \in \mathbb{N}^2 : \mathcal{O}[q^m] = \mathcal{O}[r^n] \text{ and } n \equiv \ell \pmod{R}\},$$

$$V_\ell := \{m \in \mathbb{N} : (m, n) \in W_\ell \text{ for some } n\} = \pi_1(W_\ell),$$

where  $\pi_1$  is the projection from  $\mathbb{N}^2$  onto its first factor.

Since  $q^m \notin K$  for every  $m \in \mathbb{N}$ , we have that  $W_0 = \emptyset$ . Hence it suffices to consider  $\ell > 0$ . We have the following:

**Proposition 5.1.** (a) *There is a constant  $c_{20}(d)$  such that for every  $0 < \ell \leq R-1$ , the set  $V_\ell$  has at most  $c_{20}(d)$  elements.*

(b) *Given  $\ell$  and  $m$  with  $0 < \ell \leq R-1$  and  $m \in V_\ell$ . Then either the set*

$$U_m := \{(m, n) \in W_\ell\}$$

*is a singleton or  $r^R \in \mathcal{O}^*$ .*

(c) *If  $r^R \in \mathcal{O}^*$  then for every  $0 < \ell \leq R-1$  and every  $m \in V_\ell$ , we have*

$$U_m = \{(m, \ell + jR) : j \in \mathbb{N} \cup \{0\}\}.$$

*Proof.* For part (a), we use the same arguments as in the proof of Proposition 4.4. Pick  $\sigma \in \text{Gal}(L/K)$  such that  $\sigma$  does not fix  $q^m$  for any  $m \in \mathbb{N}$ . For every  $(m, n) \in W_\ell$ , write  $n = \tilde{n}R + \ell$ . As in the proof of Proposition 4.4, we have:

$$q^m - \sigma(q^m) = u_{m, n, \sigma} r^{\tilde{n}R} (r^\ell - \sigma(r^\ell))$$

which gives at most  $c_{20}(d)$  possibilities for  $\frac{q^m}{\sigma(q^m)}$ . Hence there are at most  $c_{20}$  possibilities for  $m$  because of the choice of  $\sigma$ .

For part (b), we note that  $U_m \neq \emptyset$  since  $m \in V_\ell$ . Assume there are  $n_1 < n_2$  such that  $(m, n_1), (m, n_2) \in W_\ell$ . As before, write  $n_i = \tilde{n}_i R + \ell$  for  $i = 1, 2$ . From the equation

$$q^m - \sigma(q^m) = u_{m, n_1, \sigma} r^{\tilde{n}_1 R} (r^\ell - \sigma(r^\ell)) = u_{m, n_2, \sigma} r^{\tilde{n}_2 R} (r^\ell - \sigma(r^\ell)),$$

we have that  $r^{(\tilde{n}_2 - \tilde{n}_1)R}$  and, hence,  $r^R$  belong to  $\mathcal{O}^*$  by integral closedness of  $\mathcal{O}$ .

Part (c) is immediate since we have  $\mathcal{O}[r^n] = \mathcal{O}[r^\ell]$  if  $n \equiv \ell \pmod{R}$ .  $\square$

Proposition 5.1 finishes the case  $q^Q \notin \mathcal{O}$ .

**5.2. The case  $q^Q \in \mathcal{O}$ .** As in the proof of Theorem 1.4, we fix  $0 \leq k \leq Q - 1$  and  $0 \leq \ell \leq R - 1$  and describe the set:

$$W_{k, \ell} := \{(m, n) \in \mathbb{N}^2 : \mathcal{O}[q^m] = \mathcal{O}[r^n], m \equiv k \pmod{Q} \text{ and } n \equiv \ell \pmod{R}\}.$$

It is easy to show that  $W_{k, 0} = W_{0, \ell} = \emptyset$  if  $k \neq 0$  and  $\ell \neq 0$ . On the other hand:

$$W_{0, 0} = Q\mathbb{N} \times R\mathbb{N}.$$

Hence from now on we may assume  $k, \ell > 0$ . We also assume  $K(q^k) = K(r^\ell)$  and denote this field by  $F$  (otherwise  $W_{k, \ell} = \emptyset$ ). We have the tower of fields:

$$K \subsetneq F \subseteq L.$$

As before, for every  $(m, n) \in W_{k, \ell}$  and every  $\sigma \in \text{Gal}(L/K)$  with  $\sigma \notin \text{Gal}(L/F)$ , there is a unit  $u_{m, n, \sigma}$  (depending only on the coset  $\sigma \text{Gal}(L/F)$ ) such that:

$$q^m - \sigma(q^m) = u_{m, n, \sigma} (r^n - \sigma(r^n)).$$

Note that  $\sigma$  fixes  $q^{m-k}$  and  $r^{n-\ell}$ , we have:

$$(13) \quad \frac{q^{m-k}}{r^{n-\ell}} = u_{m, n, \sigma} \frac{r^\ell - \sigma(r^\ell)}{q^k - \sigma(q^k)}$$

which depends only on  $k, \ell$ , and the coset  $\sigma \text{Gal}(L/F)$ . If there are two distinct pairs  $(m_1, n_1)$  and  $(m_2, n_2)$  in  $W_{k, \ell}$ , equation (13) gives:

$$(14) \quad \frac{q^{m_2-m_1}}{r^{n_2-n_1}} = \frac{u_{m_2, n_2, \sigma}}{u_{m_1, n_1, \sigma}} \in \mathcal{O}^*$$

since it is a unit over  $\mathcal{O}$  (see Definition 1.1) and belongs to  $K$  due to  $Q \mid m_1 - m_2$  and  $R \mid n_2 - n_1$ .

Note that if  $r$  is a unit over  $\mathcal{O}$  then  $r^R \in \mathcal{O}^*$ , hence  $\mathcal{O}[r^n] = \mathcal{O}[r^\ell]$  for every  $n \equiv \ell \pmod{R}$ . Moreover, if  $q$  is not a unit over  $\mathcal{O}$  and  $(m_1, n_1), (m_2, n_2) \in W_{k, \ell}$  then (14) gives that  $m_1 = m_2$ . Hence we have the following:

**Proposition 5.2.** (a) *If both  $q$  and  $r$  are units over  $\mathcal{O}$  then  $W_{k, \ell}$  is either empty or has the form*

$$(k, \ell) + Q\mathbb{N} \times R\mathbb{N}.$$

(b) *If  $r$  is a unit over  $\mathcal{O}$  and  $q$  is not, then either  $W_{k, \ell}$  is empty or has the form*

$$\{(m_1, n) : n \equiv \ell \pmod{R}\}$$

*where  $m_1$  is the only positive integer such that  $\mathcal{O}[q^{m_1}] = \mathcal{O}[r^\ell]$ . A completely analogous statement holds when  $q$  is a unit over  $\mathcal{O}$  and  $r$  is not.*

- (c) Assume that neither  $q$  nor  $r$  is a unit over  $\mathcal{O}$ . If  $|W_{k,\ell}| \geq 2$  then the following holds. There is a minimal pair  $(M, N) \in \mathbb{N}^2$  satisfying  $\frac{q^{QM}}{r^{RN}} \in \mathcal{O}^*$ . For any 2 distinct pairs  $(m_1, n_1), (m_2, n_2) \in W_{k,\ell}$ , we have  $(m_2 - m_1)(n_2 - n_1) > 0$ . Moreover, we have  $\frac{m_2 - m_1}{QM} = \frac{n_2 - n_1}{RN}$  and it is an integer.

*Proof.* Perhaps only part (c) needs further explanation. The assertion  $(m_2 - m_1)(n_2 - n_1) > 0$  follows from (14) and the assumption that  $q$  and  $r$  are not unit over  $\mathcal{O}$ . The set of  $(M, N) \in \mathbb{Z}^2$  such that  $q^{QM}r^{RN} \in \mathcal{O}^*$  is a  $\mathbb{Z}$ -module of rank at most 1 since neither  $q$  nor  $r$  is a unit over  $\mathcal{O}$ .

In fact, this  $\mathbb{Z}$ -module has rank 1 and a basis  $(M, N) \in \mathbb{N}^2$  due to (14). As a consequence, for any distinct  $(m_1, n_1), (m_2, n_2) \in W_{k,\ell}$  the pair  $\left(\frac{m_2 - m_1}{Q}, \frac{n_2 - n_1}{R}\right)$  is an integral multiple of the basis  $(M, N)$ . This implies the last assertion of (c).  $\square$

*Assumption 5.3.* The following assumption is *only needed when one is concerned with the effectiveness of the results in the rest of this section*. Since  $\mathcal{O}$  is a Noetherian integrally closed domain, if  $q$  is not a unit (respectively  $r$  is not a unit), there are only finitely many minimal primes ideal  $\mathfrak{q}$  (respectively  $\mathfrak{r}$ ) containing  $q$  (respectively  $r$ ), each of the  $\mathfrak{q}$  (respectively  $\mathfrak{r}$ ) has height 1, and the localization  $\mathcal{O}_{\mathfrak{q}}$  (respectively  $\mathcal{O}_{\mathfrak{r}}$ ) is a DVR [Mat80]. For each such  $\mathfrak{q}$  (respectively  $\mathfrak{r}$ ), let  $v_{\mathfrak{q}}$  denote the corresponding valuation on  $K$  normalized so that  $v_{\mathfrak{q}}(K^*) = \mathbb{Z}$  (respectively  $v_{\mathfrak{r}}(K^*) = \mathbb{Z}$ ). We make the following assumption: it is possible to effectively determine all the minimal primes  $\mathfrak{q}$  (respectively  $\mathfrak{r}$ ) containing  $q$  (respectively  $r$ ) and to compute an extension on  $L$  for each of the valuations  $v_{\mathfrak{q}}$  (respectively  $v_{\mathfrak{r}}$ ).

*Remark 5.4.* Under Assumption 5.3, by choosing *one* minimal prime  $\mathfrak{q}$  containing  $q$  and using the valuation  $v_{\mathfrak{q}}$ , we can effectively determine the number  $m_1$  in (13). The pair  $(M, N)$  in part (c) can be determined effectively by using *all* the valuations  $v_{\mathfrak{q}}$  and  $v_{\mathfrak{r}}$ . If such pair  $(M, N)$  does not exist, then either  $W_{k,\ell} = \emptyset$  or  $W_{k,\ell}$  contains at most one element; in both cases the set  $W_{k,\ell}$  can be computed thanks to (13).

From now on, we assume that neither  $q$  nor  $r$  is a unit, there is a minimal pair  $(M, N) \in \mathbb{N}^2$  satisfying  $\frac{q^{QM}}{r^{RN}} \in \mathcal{O}^*$ , and  $W_{k,\ell} \neq \emptyset$ . Part (c) of Proposition 5.2 shows that  $W_{k,\ell}$  has the minimal element denoted  $(\tilde{m}, \tilde{n})$  such that every  $(m, n)$  in  $W_{k,\ell}$  has the form  $(\tilde{m} + tQM, \tilde{n} + tRN)$  for some  $t \in \mathbb{N} \cup \{0\}$ . We finish this section by solving the following two problems:

- I: explain how to obtain an upper bound for  $\tilde{m}$  and  $\tilde{n}$ . Once this is done, by verifying the equation  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  for  $m$  and  $n$  within such a bound, we could decide whether  $W_{k,\ell}$  is empty or not.
- II: given  $(\tilde{m}, \tilde{n})$ , explain how to find all  $t$  such that  $(\tilde{m} + tQM, \tilde{n} + tRN) \in W_{k,\ell}$ . This completely describes  $W_{k,\ell}$ .

For the rest of this section,  $c_{21}, c_{22}, \dots$  denote positive constants depending on  $K$ ,  $q$ , and  $r$ . These constants can be computed under Assumption 5.3. We have:

**Lemma 5.5.** *There is a positive constant  $c_{21} \geq 1$  such that:  $\tilde{n} \leq c_{21}\tilde{m}$  and  $\tilde{m} \leq c_{21}\tilde{n}$ .*



*Proof.* By picking one valuation  $v_q$  and one valuation  $v_r$ , we can use (13) to prove this lemma easily.  $\square$

Let  $d' := [F : K] \geq 2$ , we can uniquely write:

$$(15) \quad \begin{aligned} q^{\tilde{m}} &= a_0 + a_1 r^{\tilde{n}} + a_2 r^{2\tilde{n}} + \dots + a_{d'-1} r^{(d'-1)\tilde{n}} \\ r^{\tilde{n}} &= b_0 + b_1 q^{\tilde{m}} + b_2 q^{2\tilde{m}} + \dots + b_{d'-1} q^{(d'-1)\tilde{m}} \end{aligned}$$

for  $a_0, \dots, a_{d'-1}, b_0, \dots, b_{d'-1} \in \mathcal{O}$ . Denote  $u = \frac{q^{QM}}{r^{RN}} \in \mathcal{O}^*$ . For every  $t \in \mathbb{Z}$ , using  $q^{tQM} = u^t r^{tRN}$  and  $r^{tRN} = u^{-t} q^{tQM}$ , we have the following:

$$(16) \quad \begin{aligned} q^{\tilde{m}+tQM} &= \alpha_0 + \alpha_1 r^{\tilde{n}+tRN} + \alpha_2 r^{2(\tilde{n}+tRN)} + \dots + \alpha_{d'-1} r^{(d'-1)(\tilde{n}+tRN)} \\ r^{\tilde{n}+tRN} &= \beta_0 + \beta_1 q^{\tilde{m}+tQM} + \beta_2 q^{2(\tilde{m}+tQM)} + \dots + \beta_{d'-1} q^{(d'-1)(\tilde{m}+tQM)} \end{aligned}$$

where  $\alpha_i = \frac{a_i u^t}{r^{(i-1)tRN}} \in K$  and  $\beta_i = \frac{b_i u^{-t}}{q^{(i-1)tQM}} \in K$  for  $0 \leq i \leq d' - 1$ . Now we can give an upper bound for  $\tilde{m}$  and  $\tilde{n}$ :

**Proposition 5.6.** *Define  $c_{22} = c_{21} \max\{QM, RN\}$ . We have  $\max\{\tilde{m}, \tilde{n}\} \leq c_{22}$ .*

*Proof.* Assume otherwise:  $\max\{\tilde{m}, \tilde{n}\} > c_{22}$ . Then Lemma 5.5 gives that  $\tilde{m} > QM$  and  $\tilde{n} > RN$ . By (15) and the fact that  $\frac{q^{QM}}{r^{RN}} \in \mathcal{O}^*$ , we have that  $a_0 \in r^{RN}\mathcal{O}$  and  $b_0 \in q^{QM}\mathcal{O}$ . By (16) when  $t = -1$ , we have that  $\alpha_i, \beta_i \in \mathcal{O}$  for  $0 \leq i \leq d' - 1$ ; it suffices to check this when  $i = 0$  only. In other words, we have  $\mathcal{O}[q^{\tilde{m}-QM}] = \mathcal{O}[r^{\tilde{n}-RN}]$  violating the minimality of  $(\tilde{m}, \tilde{n})$ .  $\square$

Since we have bounded  $(\tilde{m}, \tilde{n})$  in terms of  $K$ ,  $q$ , and  $r$ , the bounds given below, which apparently depend on  $(\tilde{m}, \tilde{n})$ , indeed depend only on  $K$ ,  $q$ , and  $r$ . It is obvious that the two conditions “ $a_i \neq 0$  for some  $2 \leq i \leq d' - 1$ ” and “ $b_j \neq 0$  for some  $2 \leq j \leq d' - 1$ ” are equivalent since  $q^{\tilde{m}}$  is linear in  $r^{\tilde{n}}$  iff  $r^{\tilde{n}}$  is linear in  $q^{\tilde{m}}$ . When  $a_i = b_j = 0$  for every  $2 \leq i, j \leq d' - 1$ , the equation  $\mathcal{O}[q^{\tilde{m}}] = \mathcal{O}[r^{\tilde{n}}]$  is equivalent to  $a_1$  or  $b_1$ , hence both, are units. The following result concludes this section:

**Proposition 5.7.** *If  $d' \geq 3$  and  $a_i \neq 0$  for some  $2 \leq i \leq d' - 1$  (hence  $b_j \neq 0$  for some  $2 \leq j \leq d' - 1$ ), there exists a positive constant  $c_{23}$  such that every  $(m, n) \in W_{k,\ell}$  satisfies  $\frac{m - \tilde{m}}{QM} = \frac{n - \tilde{n}}{RN} \leq c_{23}$ . Consequently,  $W_{k,\ell}$  has at most  $c_{23} + 1$  elements.*

*On the other hand, if  $a_i = b_i = 0$  for every  $2 \leq i \leq d' - 1$  (this is vacuously true when  $d' = 2$ ), then:*

$$W_{k,\ell} = \{(\tilde{m} + tQM, \tilde{n} + tRN) : t \in \mathbb{N}\}.$$

*Proof.* To prove the first assertion, pick  $2 \leq i \leq d' - 1$  such that  $a_i \neq 0$ . By using a valuation  $v_r$ , we have that for sufficiently large  $t \in \mathbb{N}$ , the coefficient:

$$\alpha_i = \frac{a_i u^t}{r^{(i-1)tRN}}$$

cannot belong to  $\mathcal{O}$ , hence  $q^{\tilde{m}+tQM} \notin \mathcal{O}[r^{\tilde{n}+tRN}]$ .

For the second assertion, for every  $t \in \mathbb{N}$ , we have  $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathcal{O}$  while  $\alpha_i = \beta_i = 0$  for  $2 \leq i \leq d' - 1$ . This gives  $\mathcal{O}[q^{\tilde{m}+tQM}] = \mathcal{O}[r^{\tilde{n}+tRN}]$ .  $\square$

## 6. FINAL REMARKS AND FURTHER QUESTIONS

**6.1. Effectiveness of our results.** The effectiveness of Theorem 3.3 and results in Section 5 has been discussed. For Theorem 1.4 we note that it is *not* effective in the sense that we cannot provide a bound for the pairs  $(m, n) \notin \mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$  satisfying  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$ . The reason is that the theorem of Evertse, Schlickewei and Schmidt is not effective. Its proof relies crucially on a quantitative absolute version of the Subspace Theorem by Evertse and Schlickewei [ES02] after seminal work by Schmidt [Sch72], [Sch89]. The question of making the Subspace Theorem effective is still wide open. We ask the following:

**Question 6.1.** *Let  $\mathcal{O}$ ,  $q$ ,  $r$ ,  $\mathcal{A}_{\mathcal{O}, q, r}$ ,  $\mathcal{B}_{\mathcal{O}, q, r}$ ,  $\mathcal{C}_{\mathcal{O}, q, r}$  be as in Theorem 1.4. Provide a bound (depending on  $\mathcal{O}$ ,  $q$ , and  $r$ ) for all pairs  $(m, n) \in \mathbb{N}^2$  such that  $\mathcal{O}[q^m] = \mathcal{O}[r^n]$  and  $(m, n) \notin \mathcal{A}_{\mathcal{O}, q, r} \cup \mathcal{B}_{\mathcal{O}, q, r} \cup \mathcal{C}_{\mathcal{O}, q, r}$ .*

**6.2. Another result by Bell and Hare.** Besides the results mentioned previously in this paper, Bell and Hare [BH09, Theorem 1.5] prove the following:

**Theorem 6.2** (Bell-Hare). *Let  $r$  be an algebraic integer of degree at most 3. Then there are at most 40 Pisot numbers  $q$  such that  $\mathbb{Z}[q] = \mathbb{Z}[r]$ .*

They cannot find an example of  $r$  (of degree 3) that gives more than 7 Pisot numbers  $q$  satisfying  $\mathbb{Z}[q] = \mathbb{Z}[r]$ , and ask for an improvement to the bound 40. Unfortunately, the bound in Corollary 3.4 when  $\mathcal{O} = \mathbb{Z}$  and  $d = 3$  is *much larger* than 40. The proof of Theorem 6.2 uses results on cubic Thue equations  $F(x, y) = 1$  by Bennett [Ben01, Theorem 1.4].

**6.3. Another approach to Theorem 1.4.** In [BH09, Theorem 1.1], Bell and Hare actually study the equation  $\text{disc}_{\mathbb{Q}}(q^n) = \text{disc}_{\mathbb{Q}}(r^n)$ . Using Definition 2.2, they expand both sides to conclude that a certain linear recurrence sequence vanishes at  $n$ . Their definition of being “full rank” mentioned at the beginning of this paper makes it relatively easy to study the degeneracy of the resulting linear recurrence sequence.

On the other hand, we can ask the problem of describing all  $(m, n)$  such that  $\frac{\text{disc}_K(q^m)}{\text{disc}_K(r^n)} \in \mathcal{O}^*$ . Again, we can use Definition 2.2 to expand  $\text{disc}_K(q^m)$  and  $\text{disc}_K(r^n)$  and get a unit equation, then Theorem 2.3 provides a bound on the number of nondegenerate solutions. However, there are two issues. First, it does not seem entirely obvious how to get the exact relation (such as the relations described in the sets  $\mathcal{A}_{\mathcal{O}, q, r}$ ,  $\mathcal{B}_{\mathcal{O}, q, r}$ , and  $\mathcal{C}_{\mathcal{O}, q, r}$ ) from “too many” degenerate solutions. Second, by studying the property  $\frac{\text{disc}_K(q^m)}{\text{disc}_K(r^n)} \in \mathcal{O}^*$  alone, we can never rule out the case, say,  $q^m = u\sigma(r^n)$  for some conjugate  $\sigma(r^n)$  of  $r^n$  and some  $u \in \mathcal{O}^*$ . On the other hand, Theorem 1.4 indicates that (except finitely many  $(m, n)$ ) the case  $q^m = u\sigma(r^n)$  (with  $\sigma(r^n) \neq r^n$ ) can only happen when  $q^m$  and  $r^n$  have degree 2 over  $K$ .

## REFERENCES

- [Bak75] A. Baker, *Transcendental number theory*, Cambridge University Press, 1975.
- [BBM70] M. Bruckheimer, A. C. Bryan, and A. Muir, *Groups which are the union of three subgroups*, Amer. Math. Monthly **77** (1970), 52–57.

- [BC97] E. Bombieri and P. B. Cohen, *Effective diophantine approximation on  $\mathbb{G}_m$ , II*, Ann. Sc. Norm. Super. Pisa Cl. Sci. **24** (1997), 205–225.
- [Ben01] M. A. Bennett, *On the representation of unity by binary cubic forms*, Trans. Amer. Math. Soc. **353** (2001), 1507–1534.
- [BG06] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
- [BH09] J. P. Bell and K. G. Hare, *On  $\mathbb{Z}$ -modules of algebraic integers*, Canad. J. Math. **61** (2009), 264–281.
- [BH12] ———, *Corrigendum to “on  $\mathbb{Z}$ -modules of algebraic integers”*, Canad. J. Math. **64** (2012), 254–256.
- [Bom93] E. Bombieri, *Effective diophantine approximation on  $\mathbb{G}_m$* , Ann. Sc. Norm. Super. Pisa Cl. Sci. **20** (1993), 61–89.
- [BS96] F. Beukers and H. P. Schlickewei, *The equation  $x + y = 1$  in finitely generated groups*, Acta Arith. **78** (1996), 189–199.
- [BW93] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62.
- [EG85] J.-H. Evertse and K. Györy, *On unit equations and decomposable form equations*, J. Reine Angew. Math. **358** (1985), 6–19.
- [EG13] ———, *Effective results for unit equations over finitely generated domains*, Math. Proc. Cambridge Philos. Soc. **154** (2013), 351–380.
- [ES02] J.-H. Evertse and H. P. Schlickewei, *A quantitative version of the Absolute Subspace Theorem*, J. Reine Angew. Math. **548** (2002), 21–127.
- [ESS02] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2) **155** (2002), 807–836.
- [GY06] K. Györy and K. Yu, *Bounds for the solutions of  $S$ -unit equations and decomposable form equations*, Acta Arith. **123** (2006), 9–41.
- [Gyö84] K. Györy, *Effective finiteness theorem for polynomials with given discriminant and integral elements with discriminant over finitely generated domains*, J. Reine Angew. Math. **346** (1984), 54–100.
- [Lan83] S. Lang, *Fundamentals of diophantine geometry*, Springer, New York, 1983.
- [Mat80] H. Matsumura, *Commutative algebra*, second ed., Mathematics Lecture Note Series, Benjamin/Cummings Publishing Company, Reading, Massachusetts, 1980.
- [Rib01] P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer, New York, 2001.
- [Roq58] P. Roquette, *Einheiten und Divisorenklassen in endlich erzeugbaren Körpern*, Jber. Deutsch. Math. Verein **60** (1958), 1–21.
- [Sch72] W. M. Schmidt, *Norm form equations*, Ann. of Math. (2) **96** (1972), 526–551.
- [Sch89] ———, *The subspace theorem in diophantine approximations*, Compos. Math. **69** (1989), 121–173.
- [Yu07] K. R. Yu,  *$p$ -adic logarithmic forms and group varieties III*, Forum Math. **19** (2007), 187–280.

KHOA D. NGUYEN, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, AND  
 PACIFIC INSTITUTE FOR THE MATHEMATICAL SCIENCES, VANCOUVER, BC V6T 1Z2, CANADA  
*E-mail address:* `dknguyen@math.ubc.ca`  
*URL:* `www.math.ubc.ca/~dknguyen`